Undergraduate Thesis Prospectus

**Increasing Engagement in eHealth Interventions**
**Using Personalization and Implementation Intentions**
(technical research project in Engineering Systems and Environment)

**Data Laws: Regulating the Not-So-Private Private Sector**
(STS research project)

by

Judy Nguyen

May 5, 2020

technical project collaborators:
Darby Anderson
Amanda Brownlee
Camryn Burley
Georgie Lafer
Taylor Luong
Meaghan McGowan
William Trotter
Halle Wine

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

signed: _____ date: _____

approved: _____ date: _____
Peter Norton, Department of Engineering and Society

approved: _____ date: _____
Laura Barnes, Department of Engineering Systems and Environment

## General research problem

*How are data collection methods redefining 'optional'?*

Online users have seemingly free access to the web, yet the internet is a service. Services have costs. The unseen payor of cables and servers profits when anyone connects to a website, allowing data collectors to track people's virtual actions. This information is monetizable, with or without the users' knowledge or consent. Everyone is affected by data policy due the ubiquity of the internet. Even individuals who are inactive are vulnerable if tagged by family or friends. Moreover, as vital industries develop digital platforms, the internet becomes unavoidable.

## Increasing Engagement in eHealth Interventions Using Personalization and Implementation Intentions

*How can providers increase engagement and decrease attrition in eHealth interventions for socially anxious patients?*

The technical advisor is Professor Laura Barnes in the Department of Engineering Systems and Environment, and the team technical project is in collaboration with eight other undergraduates. Goals include creation of personalizable modules and goal-setting functions for individualized interventions. Our project, titled "MindTrails," is an online intervention program that uses cognitive bias modification (CBM) to alter negative interpretations of situations by participants with anxiety. The intervention consists of five levels of training sessions with a mandatory five-day break in between.

MindTrails faces high rates of attrition, partly due to lack of personalization and applicability to the patient. Targeting scenarios, rather than presenting the same situations

to every user, makes sessions more relevant to each individual. Thus, impacting the participant by centering scenarios around realistic conditions. When the user is immersed, a technique called “implementation intentions” is employed to modify cognitive behaviors by suggesting positive if-then statements that contribute to a situationally relevant goal. Incorporating implementation intentions generalizes the scenario lessons, thereby actively encouraging goal-setting applied in training to reality.

Since MindTrails is aimed at anxious users, certain strategies pursued by social media companies or video game studios to increase engagement should not be applied. Those practices aim to addict, irrespective of the mental wellness of their customers. Therefore, typical gamification methods must be evaluated for undue stress in addition to success.

Even as mental health awareness rises; the healthcare resources remain inaccessible to those in need. In 2018, 1 in 5 adults (47.6 million people) in the U.S. experienced mental illness, but less than half (43.3%) received treatment (SAMHSA). Harvey & Gumport found that the disparity between those who need treatment and those who actually receive it is due to convenience, stigmatization, and affordability (2015). Although interventions by eHealth, defined by the WHO as the use of information and communication technologies for health purposes, increase accessibility– these programs struggle to retain users throughout the course of treatment (2018). To improve online intervention retention and interaction, the technical project will research and development goal-setting and personalization methods that support participants for the duration of the study.

The capstone team will split into two subgroups: one to personalize scenarios, and the other to implement intentions and goal-setting features. Both groups will research, wireframe, and program MindTrails interfaces. In collaboration with a team of graduate psychology students, we will develop concepts for personalized scenarios and implementation intentions that the systems team will translate into mock-ups created in Figma. After gaining familiarity with Python web framework, “Flask”, and JavaScript library, “React,” we will work with a CS Capstone to incorporate the designs into the front-end. Once a minimum viable product is built, testing and refactoring the codebase will be an iterative process that will enhance results and consume the remainder of the time.

Final deliverables include a literature review on the influence of personalization and implementation intentions in an eHealth setting. Each subgroup will also produce mock-ups, feature specifications, code pushes, and sandbox prototypes for their respective focuses. The personalization team will use information collected by demographic questions already assessed upon signing up for the program, such as employment status, relationship, urban-rural classification, in order to tailor the program based on users’ responses to what domains give them anxiety. The implementation intentions team will receive scenarios from the psychology counterpart and configure them into the program, since Gollwitzer’s study proves integration will enable participants to act on the goals they set for themselves (Gollwitzer, 1999). This is valuable research and development for transitioning to a digital provider in order to increase mental health resource accessibility to individuals who need it.

**Data Laws: Regulating the Not-So-Private Private Sector**

*How are social groups competing to shape the legal standard governing online data protection?*

The slow, reactive act of lawmaking contrasts sharply with Silicon Valley's race to innovate. Legal standards governing online data protections lag, placing consumers at risk as private data stores have surpassed public records (Strickland & Hunt, 2005). Data protection laws are crucial to protecting individual rights to security and privacy.

Users have little control over the content they see. Targeted advertisements are based on age, gender, liked pages, and even browsing history (Berman, 2018). But when such marketing seems intrusive, it can backfire for the advertiser.

Users are generally also unaware of the content collected from them. Companies are disincentivized to have user-friendly Terms and Conditions. Instead, the contracts are lengthy and filled with legal jargon– or they are brief but vague to claim maximum allowances (Lomas & Dillet, 2015). Third-party companies are eager to buy this data for profitable use and distribution. These companies build detailed profiles to create a digital identity of everyone online.

Privacy and security are not necessarily mutually exclusive. Privacy in an online context "entails the protection and appropriate use of the personal information of customers, and the meeting of expectations of customers about its use (Pearson & Benameur, 2010). Internet security is more established in literature. One of the first publications on electronic commerce defines security as protection against a "circumstance, condition, or event with the potential to cause economic hardship to data

or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse" (Kalakota & Whinston, 1996).

Both security and privacy have led to data protection legislation. In 1970, Hessen, Germany was the first adopter of such statutes, when frameworks protecting personal data proved ineffective when the data moves to another jurisdiction (Phillips, 2018). Almost 50 years later, the EU passed General Data Protection Regulation (GDPR) to give users control over their personal data (Marelli & Testa, 2018).

Major participants include tech companies, social media users, privacy advocates, data brokers, advertisers, and regulators. In response to a privacy scandal, Facebook's Mark Zuckerberg said: "I started Facebook, and I'm responsible for what happens on our platform" (Salinas, 2018). Big tech is being held accountable for profitable practices, such as selling user data. To hold companies responsible, groups such as the American Civil Liberties Union endorse "Civil Rights Principles for the Era of Big Data" (Calabrese, 2014). They view privacy as a right that eager businesses infringe upon. More aggressive critics of big tech have formed an anti-social media movement. An ex-Facebooking columnist writes that mainstream social media platforms are "engineered to be addictive… as these companies gather more data about their users, it is becoming more addictive" (Mahdawi, 2018). Individuals like Mahdawi value individual liberties like security and privacy, going so far as to quit social media altogether in order to reclaim control.

The Consumer Technology Association has mobilized to represent smaller tech companies, creating a PAC that resists "design mandates that will raise costs and reduce [the] freedom to innovate" (CTA, 2019). Like tech giants, they object to regulations that

impede on profits. Data brokers are businesses that collect and sell personal information. While some let consumers see the data they collect about them, only voluntary guidelines regulate what information is used, and how (Naylor, 2016).

Data can also be mishandled or leaked to criminals. Smith et al. (2012) found that image meta-data, including GPS coordinates and facial recognition tags, can be compromised. This shields criminals engaged in fraud, theft, and blackmail. Worse still, the threat is not confined to active users. Inactive persons are exposed when family or friends mention them online. The internet has no borders, limiting the effect of national laws. Nonetheless, European Union (EU) laws seek to "protect all EU citizens from privacy and data breaches," and they affect all companies that do business with its residents (EU GDPR, 2019).

Although national laws vary, Reidenberg (2000) contends that the world's democracies recognize "information privacy as a critical element of civil society." As more citizens of the world get connected, the amount of data gleaned from online users continues to grow.

## References

Berman, R. (2018). Beyond the Last Touch: Attribution in Online Advertising. *Marketing Science*, *37*(5), 771–792. https://doi.org/10.1287/mksc.2018.1104

Calabrese, C. (2014, February 27). When Big Data Becomes a Civil Rights Problem. https://www.aclu.org/blog/smart-justice/mass-incarceration/when-big-data-becomes-civil-rights-problem

CTA. (2019). Consumer Technology Association Political Action Committee (CTAPAC). https://www.cta.tech/Policy/CTAPAC.aspx

EU GDPR. (2019). European Union General Data Protection Regulation. https://eugdpr.org/the-regulation/

Gollwitzer, P. M. (1999). Implementation Intentions: Strong Effects of Simple Plans. *American Psychologist*, 11.

Harvey, A. G., & Gumport, N. B. (2015). Evidence-based psychological treatments for mental disorders: Modifiable barriers to access and possible solutions. *Behaviour Research and Therapy*, *68*, 1–12. https://doi.org/10.1016/j.brat.2015.02.004

Lomas, N., & Dillet, R. (2015, August 21). Terms And Conditions Are The Biggest Lie Of Our Industry. http://social.techcrunch.com/2015/08/21/agree-to-disagree/

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation. *Science*, *360*(6388), 496–498. https://doi.org/10.1126/science.aar5419

Naylor, B. (2016, July 11). Firms Are Buying, Sharing Your Online Info. What Can You Do About It? https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it

Pearson, S., & Benameur, A. (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. *2010 IEEE Second International Conference on Cloud Computing Technology and Science*, 693–702. https://doi.org/10.1109/CloudCom.2010.66

Phillips, M. (2018). International data-sharing norms: From the OECD to the General Data Protection Regulation (GDPR). *Human Genetics*, *137*(8), 575–582. https://doi.org/10.1007/s00439-018-1919-7

Ravi Kalakota, & Whinston, A. B. (1996). *Frontiers of Electronic Commerce*. https://books.google.com/books/about/Frontiers_of_Electronic_Commerce.html?id=ckhPAAAAMAAJ

Reidenberg, J. R. (2000). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Review*, *52*(5), 1315–1371. https://doi.org/10.2307/1229516

Salinas, S. (2018, March 21). Zuckerberg on Cambridge Analytica: "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you." https://www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html

SAMHSA. (2018). Key Substance Use and Mental Health Indicators in the United States: Results from the 2018 National Survey on Drug Use and Health. *Substance Abuse and Mental Health Services Administration (SAMHSA)*, 82.

Smith, M., Szongott, C., Henne, B., & Voigt, G. von. (2012). Big Data Privacy Issues in Public Social Media. *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, 1–6. https://doi.org/10.1109/DEST.2012.6227909

Strickland, L. S., & Hunt, L. E. (2005). Technology, security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology*, *56*(3), 221–234. https://doi.org/10.1002/asi.20122

WHO. (2018). World Health Organization. EHealth at WHO. http://www.who.int/ehealth/about/en/